

User guide for Kingston Data Traveler Locker + G2

Initial configuration

These instructions are for Windows XP and Windows 7 devices but the principles will be the same for other operating systems.

The encrypted USB stick must be configured with a password before it can be used. You must remember this password in order to access any data stored on the USB stick. Please note: There is no backup or recovery mechanism for this password.

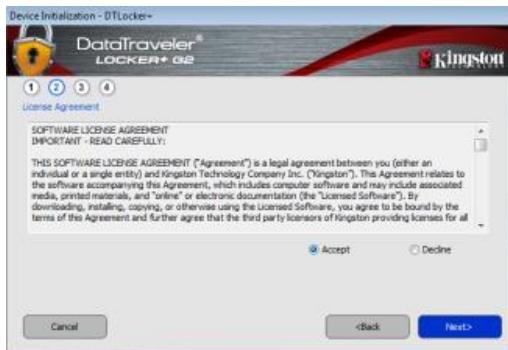
When you connect the encrypted USB stick to your PC or laptop for the first time, the following window will be displayed.



Run DTLplus_Launcher.exe should be highlighted and this is the option to run. The following window will be displayed:



Select the language you wish to use with the device. *English* should be displayed by default. Then click **Next>** to display the following window:



Read the software license agreement, click **Accept** to accept it and then click **Next>** to display the following window:



Your password must be at least 8 characters long and contain three of the following types of characters: upper case, lower case, numbers and special characters. If you forget this password you will no longer be able to access the data on the USB stick, so do make use of the *Hint:* field to provide information about the password. Do not make the hint so obvious that someone finding the USB stick would be able to guess the password.

Note: Once the configuration process has finished, you cannot change your password without deleting all the data from your USB stick.

Create a password for this USB stick by entering the same password twice in the appropriate fields.

Click **Next>** to display the following window:



Enter **your name** and **University of Exeter** or your department so that the device may be returned to you if found. Then click **Finish** to encrypt the USB stick.



When this process has finished the **OK** button will be available.



Click **OK** to close the window.

From now on you will have to enter the password to access any files or data copied onto the USB stick.

Safely remove the USB stick as usual.

The next time you connect the USB stick to your PC or laptop, the following window should be displayed:



Enter your password and click **Login**. You will then be able to read from and write to the USB stick normally.

Windows 7 autorun feature

If you are using the USB stick on a Windows 7 machine, the next time you connect the encrypted USB stick to your device instead of the DTLPlus_Launcher application

automatically starting with a prompt for you to enter your password, the following window is displayed again:



If you do not want to have to select this option each time you connect the encrypted USB stick, you can select the *Always do this for software and games:* checkbox and then click **Run DTLplus_Launcher.exe**. If this application is present on a connected USB device it will be automatically run.

This window should be displayed:



The next time you connect the encrypted USB stick to this Windows 7 PC or laptop, the 'enter password' applications should automatically start.

Failed login attempts

If you enter your password incorrectly, a message indicating that there was a failed login attempt is displayed:



Note: You have up to 10 attempts to enter your password correctly. Once the password is entered correctly, the counter is reset to 10. Select **Show Password Hint** to view the information you set previously about this password. If you cannot remember the password

after 10 attempts, you will have to re-encrypt the USB stick with a new password and all files and data present on the USB stick will be lost.

Further Information

For other information about the USB stick please see our FAQ.